

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005859
(43)Date of publication of application : 08.01.2003

(51)Int.Cl. G06F 1/00
G06F 9/445
G06F 15/00

(21)Application number : 2001-216467 (71)Applicant : SUMIYA YUICHI
(22)Date of filing : 17.07.2001 (72)Inventor : SUMIYA YUICHI

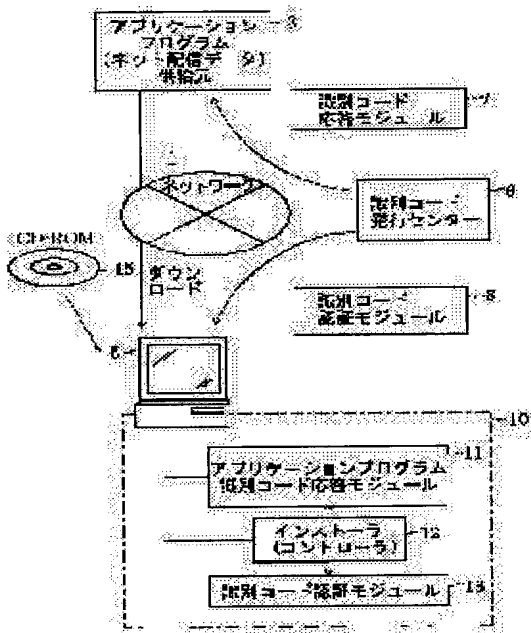
(30)Priority
Priority number : 2001116516 Priority date : 16.04.2001 Priority country : JP

(54) METHOD FOR MANAGING PROGRAM AND DATA, AND COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an application program from being unauthorizedly copied by preventing the application program from being installed by any one other than a client who has made an official purchase agreement for the program.

SOLUTION: Even when the application program and data are downloaded to a terminal 5, it is made impossible to use them as they are. Unique identification codes that do not overlap on one another are allocated to all application programs, and an identification code response module 7 that responds with the identification codes as a key is incorporated into the application program, the program is provided to an application program supply source 3. An identification code authentication module 8 executes an authentication processing responding to an identification code authentication module 13 in a terminal 5.



LEGAL STATUS

- [Date of request for examination]
- [Date of sending the examiner's decision of rejection]
- [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
- [Date of final disposal for application]
- [Patent number]
- [Date of registration]
- [Number of appeal against examiner's decision of rejection]
- [Date of requesting appeal against examiner's decision]

of rejection]
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-5859

(P2003-5859A)

(43) 公開日 平成15年1月8日 (2003.1.8)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 1/00		G 0 6 F 15/00	3 3 0 A 5 B 0 7 6
9/445		9/06	6 6 0 G 5 B 0 8 5
15/00	3 3 0		6 4 0 A
			6 1 0 L

審査請求 未請求 請求項の数14 O L (全 16 頁)

(21) 出願番号 特願2001-216467 (P2001-216467)

(22) 出願日 平成13年7月17日 (2001.7.17)

(31) 優先権主張番号 特願2001-116516 (P2001-116516)

(32) 優先日 平成13年4月16日 (2001.4.16)

(33) 優先権主張国 日本 (J P)

(71) 出願人 301038726

角谷 優一

東京都杉並区高井戸東3丁目14番29号

(72) 発明者 角谷 優一

東京都杉並区高井戸東3丁目14番29号

(74) 代理人 100102923

弁理士 加藤 雄二

Fターム (参考) 5B076 BB06 FB02

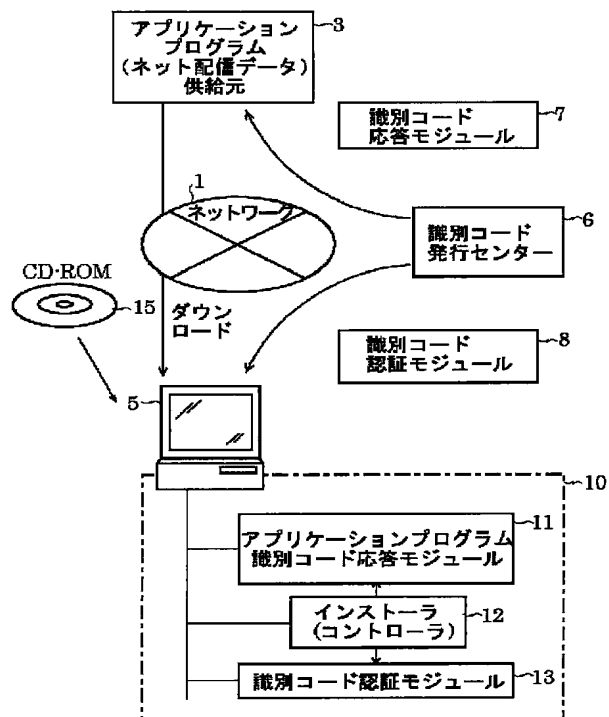
5B085 AA08 AE23 BG06

(54) 【発明の名称】 プログラムやデータの管理方法とコンピュータ

(57) 【要約】

【解決手段】 アプリケーションプログラムやデータを端末5にダウンロードしても、そのままでは使用できないようにする。全てのアプリケーションプログラムに対し、互いに重複しないユニークな識別コードを割り付、その識別コードをキーとして応答する識別コード応答モジュール7を組み込む。アプリケーションプログラム供給元3に対して提供する。識別コード認証モジュール8は、端末5において、識別コード認証モジュールに回答して認証処理を実行する。

【効果】 正式にプログラムの購入契約をしたクライアント以外はアプリケーションプログラムのインストールができないので、不正コピーを防止できる。



(2)

1

【特許請求の範囲】

【請求項1】 コンピュータ上で動作するアプリケーションプログラムに、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記アプリケーションプログラムをインストールされるコンピュータ上で、前記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと前記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、インストーラに前記アプリケーションプログラムのインストールを実行させることを特徴とするアプリケーションプログラムのインストール管理方法。

【請求項2】 コンピュータにダウンロードされる任意のデータ群に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記データ群をダウンロードされるコンピュータ上で、前記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと前記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、コントローラに前記データ群のダウンロードを実行させることを特徴とするデータ群のダウンロード管理方法。

【請求項3】 予めコンピュータに登録されたアプリケーションプログラムが、予めそのコンピュータに登録された識別コードを付加したコマンドを発行した場合にのみ、そのコンピュータ上での当該コマンドの実行を許可する識別コード認証モジュールを備えたことを特徴とするコンピュータ。

【請求項4】 請求項3に記載のコンピュータにおいて、識別コード認証モジュールは、任意のタイミングで、アプリケーションプログラムに対して登録された識別コードを別の識別コードに更新することを特徴とするコンピュータ。

【請求項5】 一定の重複しないユニークな識別コードであって、予め登録したものを付加したデータを使用したアクセスのみを許可するデータアクセス管理モジュールを備えたことを特徴とするコンピュータ。

【請求項6】 コンピュータと所定の情報交換処理を実行する媒体に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、

前記媒体を前記コンピュータに接続したとき、前記媒体に対応する識別コードをコンピュータに登録して管理する識別コード認証モジュールをコンピュータ上で動作させ、この識別コード認証モジュールと前記識別コード応答モ

2

ジュールの通信により、媒体中の識別コード応答モジュールに割りつけられた識別コードと、その媒体に対応する登録された識別コードの一致が確認されたときにのみ、前記情報交換処理を実行させることを特徴とする情報交換処理の管理方法。

【請求項7】 請求項6に記載の管理方法において、識別コード認証モジュールは、情報交換処理が終了したタイミングで、前記媒体の識別コード応答モジュールを、これまでとは別のユニークな新たな識別コードを割り付けたものに更新するとともに、コンピュータにその新たな識別コードを、当該媒体に対応するものとして登録することを特徴とする情報交換処理の管理方法。

【請求項8】 コンピュータにインストールしようとする情報が記録された記憶媒体には、認証用データをやりとりして認証処理を実行する機能を持つ応答モジュールが記録され、

前記情報をインストールするコンピュータは、前記応答モジュールと認証用データをやりとりして認証処理を実行する機能を持つ認証モジュールと、認証処理が正常に終了したとき、前記記憶媒体に記憶された情報をコンピュータにインストールするインストーラとを備え、少なくとも前記認証モジュールは、ネットワークを通じて認証モジュール配信用サーバからダウンロードされることを特徴とする情報のコンピュータへのインストール方法。

【請求項9】 請求項8に記載のインストール方法において、認証モジュール配信用サーバに対して認証モジュールのダウンロードを要求する機能を持つ配信要求モジュールを備えることを特徴とする情報のコンピュータへのインストール方法。

【請求項10】 請求項8に記載のインストール方法において、認証モジュール配信用サーバには、認証モジュールの配信履歴データを記録する配信記録部が備えられていることを特徴とする情報のコンピュータへのインストール方法。

【請求項11】 請求項8に記載のインストール方法において、認証モジュールは、コンピュータに正常に情報のインストールが終了すると無効化されることを特徴とする情報のコンピュータへのインストール方法。

【請求項12】 カードを使用して自動的に所定の取引を実行する自動取引装置において、前記カードには、入力データを所定のアルゴリズムで変換して識別コードを発生する第1の識別コード発生モジュールと、この第1の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを前記第1の識別コード発生モジュールに入力する第1の識別コードレジスタとが設けられ、

(3)

3

前記ATMには、入力データを前記第1の識別コード発生モジュールと同一のアルゴリズムで変換して識別コードを発生する第2の識別コード発生モジュールと、この第2の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを前記第2の識別コード発生モジュールに入力する第2の識別コードレジスタと、前記第1の識別コード発生モジュールの出力した識別コードと前記第2の識別コード発生モジュールの出力した識別コードとが一致したかどうかを判定して認証処理をする認証モジュールが設けられ定ることを特徴とする自動取引装置の認証処理方法。

【請求項13】 請求項12に記載の自動取引装置の認証方法において、

前記第1の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第1の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生し、

前記第2の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第2の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生することを特徴とする自動取引装置の認証処理方法。

【請求項14】 コンピュータに設けられた監視モジュールであって、予め管理テーブルに認証コードが登録されたアプリケーションによる要求のみをオペレーティングシステムに伝えるように動作し、ネットワークに接続されたネットワークインターフェイスを通じて、予め特定された記憶領域にデータが書き込まれる処理は前記監視モジュールの監視外に置くように、コンピュータを動作させるコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータにインストールするプログラムやコンピュータに記憶させるデータファイルなどの安全性や信頼性を確保するプログラムやデータの管理方法とこの管理を実行するコンピュータに関する。

【0002】

【従来の技術】

【0003】コンピュータシステムで、セキュリティを脅かすものには、情報の盗聴、システムやプライベートなネットワークへの侵入、本人のなりすまし、データの改竄、データやシステムの破壊といったものがあげられる。コンピュータをインターネットに接続して、情報の入手、発信、やり取り等を行うということは、プライベートな自らのネットワークやコンピュータシステムを不特定多数の者に開放して、アクセスされる危険にさらすことになる。また、自分からの情報を見ず知らずの者に伝送してしまう危険にさらすことになる。

4

【0004】コンピュータシステムへの侵入者は、ネットワークを通じてコンピュータに保管されているデータを盗み出したり、データの消去、内容の書き換えなどを行う。また、内部ネットワークシステムそのものの機能を破壊し、データ通信やコンピュータを使った業務を妨害するための侵入も企てることがある。さらに、進入したコンピュータを、ある通信ネットワークを攻撃するための、前線基地として使うこともある。

【0005】こうした危険からコンピュータを守るために、IDとパスワードを使用する方法、ファイアウォールを設ける方法、情報の暗号化をする方法、デジタル署名を利用する方法、ワンタイムパスワードを使用する方法、アクセス権の制御をする方法、ウイルスワクチンを用意する方法等が利用されている。

【0006】

【発明が解決しようとする課題】ところで、上記のような従来の技術には、次のような解決すべき課題があった。

【0007】ユーザー名(ID)とパスワードは、不正アクセスを防止するために、コンピュータに正規の利用者であることを判別させるために使用されている。ユーザー名は宛先識別用に自由に使われる。しかし、パスワードは、本人以外は知らないということを前提として使用される。ここで侵入者がいったんユーザー名とパスワードとを盗むことに成功すると、いつでも正式な利用者に成りすまして堂々とコンピュータシステムにアクセスでき、データの盗難、改竄、破壊がいとまやすく実行できるという問題がある。

【0008】ファイアウォールは、ネットワークの内部と外部との間にあって、情報の出入りを見張る。これは、入ってくる情報と出ていく情報の双方をチェックし、通過させてよい情報といけな情報を選択する役目を持つ。また、アクセスの全記録を残す機能を持ち、問題が発生したときの対策を講じることがでる。しかしながら、ファイアウォールも内部LANに接続したコンピュータのひとつで、処理速度がLAN全体に影響を与える。また、チェック機能と処理速度のバランスが実用に耐えるものでなければならない。しかも、システム内部に侵入してしまったウイルス等には対応できない。

【0009】既に開発された公開鍵、秘密鍵といった暗号化鍵を使用した方法によれば、通信中の情報の盗聴を効果的に防止することが可能である。しかしながら、鍵を盗まれないように管理が必要なこと、多数のメンバー相互間や、次々に相手が変わる不特定の相手とのやり取りには向かないという問題がある。デジタル署名も暗号化技術を発展させたもので、多数のメンバー相互間や、次々に相手が変わる不特定の相手とのやり取りには向かないという問題は解決されない。

【0010】ワンタイムパスワードは、二度繰り返して使うことができない一度限りのパスワードである。アク

(4)

5

セスのたびにパスワードが変わるので、盗難にあっても、次回以降は使えないという点で、一般のパスワードより安全性は高い。しかし、用途が限定され、パスワードの管理が煩雑になるという問題がある。

【0011】アクセス権の制御は、オペレーティングシステムに記憶装置等へのアクセスの際にパスワードの入力を要求する機能を持たせたもので、ユーザー名（ID）とパスワードを使用する方法における問題点を解決するものではない。

【0012】ウイルス対策としてウイルスチェッカやワクチンソフトを使用する方法は、既知のコンピュータウイルスの侵入を阻止してその機能を停止させることができて、未知のコンピュータウイルスには効果がないという問題がある。すなわち、ウイルスプログラムと正常のプログラムとの区別がつかなければ感染を防止できないという問題がある。

【0013】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成1〉コンピュータ上で動作するアプリケーションプログラムに、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記アプリケーションプログラムをインストールされるコンピュータ上で、上記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、インストーラに上記アプリケーションプログラムのインストールを実行させることを特徴とするアプリケーションプログラムのインストール管理方法。

【0014】〈構成2〉コンピュータにダウンロードされる任意のデータ群に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記データ群をダウンロードされるコンピュータ上で、上記識別コードと同一の識別コードを割り付けた識別コード認証モジュールを動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により識別コードの一致が確認されたときにのみ、コントローラに上記データ群のダウンロードを実行させることを特徴とするデータ群のダウンロード管理方法。

【0015】〈構成3〉予めコンピュータに登録されたアプリケーションプログラムが、予めそのコンピュータに登録された識別コードを付加したコマンドを発行した場合にのみ、そのコンピュータ上での当該コマンドの実行を許可する識別コード認証モジュールを備えたことを特徴とするコンピュータ。

【0016】〈構成4〉構成3に記載のコンピュータにおいて、識別コード認証モジュールは、任意のタイミングで、アプリケーションプログラムに対して登録された識別コードを別の識別コードに更新することを特徴とす

6

るコンピュータ。

【0017】〈構成5〉一定の重複しないユニークな識別コードであって、予め登録したものを付加したデータを使用したアクセスのみを許可するデータアクセス管理モジュールを備えたことを特徴とするコンピュータ。

【0018】〈構成6〉コンピュータと所定の情報交換処理を実行する媒体に、重複しないユニークな識別コードを割り付けた識別コード応答モジュールを含めておくとともに、上記媒体を上記コンピュータに接続したとき、上記媒体に対応する識別コードをコンピュータに登録して管理する識別コード認証モジュールをコンピュータ上で動作させ、この識別コード認証モジュールと上記識別コード応答モジュールの通信により、媒体中の識別コード応答モジュールに割りつけられた識別コードと、その媒体に対応する登録された識別コードの一致が確認されたときにのみ、上記情報交換処理を実行させることを特徴とする情報交換処理の管理方法。

【0019】〈構成7〉構成6に記載の管理方法において、識別コード認証モジュールは、情報交換処理が終了したタイミングで、上記媒体の識別コード応答モジュールを、これまでとは別のユニークな新たな識別コードを割り付けたものに更新するとともに、コンピュータにその新たな識別コードを、当該媒体に対応するものとして登録することを特徴とする情報交換処理の管理方法。

【0020】〈構成8〉コンピュータにインストールしようとする情報が記録された記憶媒体には、認証用データをやりとりして認証処理を実行する機能を持つ応答モジュールが記録され、上記情報をインストールするコンピュータは、上記応答モジュールと認証用データをやりとりして認証処理を実行する機能を持つ認証モジュールと、認証処理が正常に終了したとき、上記記憶媒体に記憶された情報をコンピュータにインストールするインストーラとを備え、少なくとも上記認証モジュールは、ネットワークを通じて認証モジュール配信用サーバからダウンロードされることを特徴とする情報のコンピュータへのインストール方法。

【0021】〈構成9〉構成8に記載のインストール方法において、認証モジュール配信用サーバに対して認証モジュールのダウンロードを要求する機能を持つ配信要求モジュールを備えることを特徴とする情報のコンピュータへのインストール方法。

【0022】〈構成10〉構成8に記載のインストール方法において、認証モジュール配信用サーバには、認証モジュールの配信履歴データを記録する配信記録部が備えられていることを特徴とする情報のコンピュータへのインストール方法。

【0023】〈構成11〉構成8に記載のインストール方法において、認証モジュールは、コンピュータに正常に情報のインストールが終了すると無効化されることを特徴とする情報のコンピュータへのインストール方法。

(5)

7

【0024】〈構成12〉カードを使用して自動的に所定の取引を実行する自動取引装置において、上記カードには、入力データを所定のアルゴリズムで変換して識別コードを発生する第1の識別コード発生モジュールと、この第1の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを上記第1の識別コード発生モジュールに入力する第1の識別コードレジスタとが設けられ、上記ATMには、入力データを上記第1の識別コード発生モジュールと同一のアルゴリズムで変換して識別コードを発生する第2の識別コード発生モジュールと、この第2の識別コード発生モジュールの出力する識別コードを保持して、次のタイミングで、保持していた識別コードを上記第2の識別コード発生モジュールに入力する第2の識別コードレジスタと、上記第1の識別コード発生モジュールの出力した識別コードと上記第2の識別コード発生モジュールの出力した識別コードとが一致したかどうかを判定して認証処理をする認証モジュールが設けられ定ることを特徴とする自動取引装置の認証処理方法。

【0025】〈構成13〉構成12に記載の自動取引装置の認証方法において、上記第1の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第1の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生し、上記第2の識別コード発生モジュールは、認証処理開始直前に入力されたパスワードと第2の認証コードレジスタに保持された認証コードを受け入れて、新たな認証コードを発生することを特徴とする自動取引装置の認証処理方法。

【0026】〈構成14〉コンピュータに設けられた監視モジュールであって、予め管理テーブルに認証コードが登録されたアプリケーションによる要求のみをオペレーティングシステムに伝えるように動作し、ネットワークに接続されたネットワークインターフェイスを通じて、予め特定された記憶領域にデータが書き込まれる処理は前記監視モジュールの監視外に置くように、コンピュータを動作させるコンピュータプログラム。

【0027】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。図1は本発明のプログラムやデータの管理方法を実施するためのシステムブロック図である。図のネットワーク1には、アプリケーションプログラムやネット配信データの供給元3のコンピュータやサーバが接続されている。また、ネットワーク1には任意のクライアントの端末5が接続されている。この端末5は、パーソナルコンピュータやモバイルコンピュータその他様々な任意のコンピュータである。ネットワーク1はデータやプログラムを転送できるものであればなんでもよいが、例えば、インターネットやイントラネットなどのネットワークである。このようなシステムでは、端末5はネットワーク1を通じてアプリケーションプログ

8

ラムやネット配信データを取得することができる。

【0028】しかしながら、こうしたシステムを利用すれば、ダウンロードされたアプリケーションプログラムやネット配信データをそのまま別の端末に転送し、別の端末で不正使用することが可能になる。すなわち、そのまま使用できるような状態でアプリケーションプログラムやデータをネットワーク1を通じて配信すると、供給元は、プログラムやデータの著作権を確実に守ることが難しいという問題があった。

10 【0029】この発明では、アプリケーションプログラムやデータを端末5にダウンロードしても、そのままでは使用できないようにする。またあるいは、正規の許可を得ない限り、ダウンロードができないようにする。このために、例えば、識別コード発行センター6を設ける。この識別コード発行センター6は、アプリケーションプログラム供給元3から供給される全てのアプリケーションプログラムに対し、互いに重複しないユニークな識別コードを割り付ける。そして、その識別コードをキーとして応答する識別コード応答モジュール7をアプリケーションプログラム供給元3に対して提供する。

20 【0030】この識別コード応答モジュール7は、アプリケーションプログラムに組み込まれる。識別コード応答モジュール7は、例えば、問い合わせコマンドに割りつけられた識別コードを付加して問い合わせをすると、「GOOD」という意味の応答を出力し、その他の場合には、「NG」という意味の応答を出力するように機能するコンピュータプログラムである。識別コード応答モジュール7は、割りつけられた識別コードを表示する機能を持つものであれば、何でも良いが、アプリケーションプログラム側から識別コードを出力させないようにしたほうが、不正コピーの防止にはより効果的である。

30 【0031】さらに識別コード発行センター6は、クライアントの端末5がアプリケーションプログラムのダウンロードを要求するとき、上記の識別コード応答モジュールと同一の識別コードを割り付けられた識別コード認証モジュールを供給クライアント側に供給する。クライアントは、例えば、予めアプリケーションプログラムの購入契約をして、識別コード認証モジュールの供給を受ける権利を獲得する。識別コード発行センター6は、識別コード認証モジュール8をネットワーク1を通じて端末5に送信する。この識別コード認証モジュール8は、端末5の所定の記憶領域書き込まれて、ダウンロードされたアプリケーションプログラムをインストールする際に、後で説明する認証処理を実行する。

40 【0032】この識別コード認証モジュール8を端末5に送り込む方法は、識別コード発行センター6がネットワーク1を通じて直接端末5に転送する以外にもある。例えば、アプリケーションプログラム供給元3が、識別コード発行センター6から供給された識別コード認証モジュール8を、ネットワーク1を通じて端末5に送り込

50

(6)

9

む方法がある。ただし、アプリケーションプログラムとは別の方法で別のタイミングで送り込むようにしないと、アプリケーションプログラムとは別に識別コード認証モジュール8を用意して配布する効果が小さくなる。アプリケーションプログラムと識別コード認証モジュール8とを一緒にコピーすれば、不正コピーが可能になるからである。従って、例えば、アプリケーションプログラムの購入契約成立時に、クライアントが意識しない状態で、クライアントの端末に識別コード認証モジュール8をダウンロードするようにすることが好ましい。

【0033】また、上記の例では、ネットワーク1を通じてアプリケーションプログラムをクライアントの端末にダウンロードする例を示して説明をしたが、アプリケーションプログラムがCD-ROM15などの媒体に記録されていたとしても同様の処理が可能である。この場合には、必ず、識別コード認証モジュール8を全く別のルートで端末5に送り込むようにする。

【0034】端末5にアプリケーションプログラムがダウンロードされ、インストールを開始すると、図1に示した1点鎖線の中に示すようなプログラムやモジュールが、端末5上で起動される。アプリケーションプログラム識別コード応答モジュール11は、ダウンロードされたアプリケーションプログラムのものである。インストーラ12は、アプリケーションプログラムをインストールして使用可能にするためのセットアップ制御を行うプログラムである。識別コード認証モジュール13は、識別コード発行センター6から端末5に対して供給を受けたプログラムモジュールである。

【0035】図2は、上記のアプリケーションプログラム識別コード応答モジュール11とインストーラ12と識別コード認証モジュール13の動作を示すシーケンスチャートである。このシーケンスが開始される前に、予め、図1に示す端末5に対しアプリケーションプログラムがダウンロードされ、さらに識別コード認証モジュール8が端末5の所定の記憶領域上に記憶されているものとする。ここで、アプリケーションプログラムのセットアップのためにインストーラ12を起動する(ステップS1)。このときインストーラ12は、識別コード認証モジュール13に対し、認証依頼を行う(ステップS2)。識別コード認証モジュール13は、ステップS3において認証用の識別コードを発生する(ステップS3)。この識別コードは、ダウンロードされたアプリケーションプログラムの識別コード応答モジュール7に割り付けられたものと同一のものである。

【0036】識別コード認証モジュール13は、発生させた識別コードを付加した問い合わせコマンドを識別コード応答モジュール11に対して送信する(ステップS4)。識別コード応答モジュール11は、この識別コードのチェックを行う(ステップS5)。自分に割り付けられた識別コードと同一の識別コードを付加した問い合

10

わせコマンドが入力した場合には、識別コードが一致したという応答を行う。また、それ以外の場合には、識別コードが不一致であるという応答を行う。ステップS6でこのような応答があると、識別コード認証モジュール13は、識別コードが一致したときにはステップS7からステップS8に進み、インストーラ12に対し、インストールの続行指示をする。それ以外の場合には、ステップS12でエラー処理を行なう。

【0037】識別コード認証モジュール13からインストールの続行指示がインストーラ12に送られると、インストーラ12では、ダウンロードされたプログラムのインストールを実行する(ステップS9)。こうしてプログラムのインストールが完了する。インストールが完了すると、インストーラ12は、識別コード認証モジュール13に対し、インストール処理の完了通知を送る(ステップS10)。識別コード認証モジュール13は、その後のアプリケーションプログラムの実行監視のために、アプリケーション管理テーブルを生成する(ステップS11)。このアプリケーション管理テーブルは、図1に示した端末5の所定の不揮発性メモリに記録され、アプリケーションプログラムが動作するときに、後で説明するような要領で動作管理を行う。

【0038】上記の方法によれば、図1に示すアプリケーションプログラム供給元3から端末5に対してダウンロードされたアプリケーションプログラムを、そのまま別のコンピュータにコピーしたとしても、識別コード認証モジュールが動作しないため、インストールをしてセットアップをすることができない。すなわち正式にプログラムの購入契約をしたクライアント以外はアプリケーションプログラムのインストールができないので、不正コピーを防止できる。なお、上記の方法によって管理できるのはアプリケーションプログラムに限らない。ネットワークを通じて配信される様々なデータ、例えば、音楽データ、書籍データなどについても同様のことが言える。もちろん、他の媒体例えば、フロッピー(登録商標)ディスクやCD-ROMやメモリカードによって配布される任意のデータについても同様である。これらのデータは予め所定の識別コード応答モジュールを組み込んで配信されるようにしておく。識別コード認証モジュール8は、実際にそのデータを使用する権利を、例えば有償で獲得したクライアントの端末に、別ルートで供給する。これで、アプリケーションプログラムの不正コピーなどを防止することが可能になる。

【0039】また、例えば、予め所定の識別コードを割り付けたプログラムやデータや各種著作物を記憶させたCD-ROMをダイレクトメールや雑誌の付録などによって提供する。しかしながら、インストール処理を実行しなければ、これらは利用できないようにしておく。その状態は、図1に示す端末5にアプリケーションプログラムやデータがダウンロードされたのと同様の状態であ

(7)

11

る。ここで、クライアントの端末5のユーザーが、ネットワーク1を通じて、例えばそのCD-ROMのシリアル番号などとCD-ROMに記録された自分の利用したいプログラムの名称などをアプリケーションプログラム供給元3に通知する。そこで代金の決済が終了すれば、そのCD-ROMのシリアル番号に基づいて、CD-ROMに記録したアプリケーションプログラムに割り付けられた識別コードを調べて、対応する識別コード認証モジュールを、クライアントの端末5に送る。

【0040】これで図2に示した通りの処理が可能になる。さらに、上記の例では、識別データを利用して、コンピュータにコピーされ、あるいはダウンロードされたプログラムやデータの使用を可能にするかどうかの管理をしたが、コンピュータにコピーやダウンロードを許可するかどうかの管理を行なうようにしてもよい。

【0041】上記の識別コードは、識別コード発行センターでなく、アプリケーションプログラムの供給元で発行することも可能である。しかしながら、いかなる場所いかなる環境においても重複しない識別コードが利用されることがこのシステムの安全な運用に結びつく。従って、識別コード発行センター6を設け、全てのアプリケーション供給元や音楽配信会社などが、この識別コード発行センター6に識別コードの発行を依頼するようなシステムが好ましい。こうすれば、常にユニークな識別番号を継続的に発行し、信頼性の高い管理が可能になる。

【0042】なお、識別コード認証モジュール8をコンピュータから取り出してダウンロードされたアプリケーションプログラムと共にコピーすれば、アプリケーションプログラムの不正コピーが可能になる。そこで、例えば識別コード認証モジュールは一度インストールを実行した後は、例えばインストーラ12によって削除されるという方法も採用できる。これによってアプリケーションプログラムのインストールを1回だけに制限することが可能になる。アプリケーションプログラムの修復などについては、ネットワークを通じて供給元が十分なサポートをすればよい。

【0043】図3の(a)は、コンピュータにインストールされたアプリケーションプログラムの動作を制限してセキュリティを高める管理方法の説明図で、(b)はその動作フローチャートである。図2のステップS11でアプリケーションプログラムのインストールが終了すると、識別コード認証モジュール13がコンピュータ中にアプリケーション管理テーブルを生成するようにした。アプリケーション管理テーブルは、図3に示すように、アプリケーションの名称27と識別コード28とを対応付けたものである。この識別コード28は、アプリケーションプログラムのインストールをする際に使用した識別コードとは全く異なるものであってよい。この例では、インストールされたアプリケーションプログラム21は、動作をする際に発行するコマンド22に、常に

12

一定の識別コード23を付加する。コマンド22はOS(オペレーティングシステム)に送り込まれる際に、まず、シェル24の部分で解釈され、その解釈の結果がカーネル25に転送される。

【0044】このシェル24でコマンド22を解析する際に、どのアプリケーションプログラムから発行されたコマンドかを判断する。同時に付加された識別コードを取得する。そして、アプリケーション管理テーブル26を参照し、そのアプリケーションプログラムがどの識別コードを付加してコマンドを発生するかを調べる。シェル24は、アプリケーションプログラム21が、アプリケーション管理テーブル26に登録された通りの識別コード28をコマンド22に付加して発行した場合にのみ、コマンド22を解釈して、カーネル25に転送するようにする。正規の手順を経ないでインストールされたアプリケーションプログラムは、アプリケーション管理テーブル26に登録されない。また、ネットワーク等を通じてコンピュータに侵入した不正なコマンドは必要な識別コードが付加されていない。従って、そのコマンドはシェルにより処理を拒絶され、OSに転送されないから、実行されることがない。すなわち、特定の登録されたアプリケーションプログラム以外はそのコンピュータ上で全く動作しないという環境が設定できる。従って、極めて安全性の高いシステムが確立される。

【0045】図3の(b)を用いて、具体的なコマンド解釈動作を説明する。まず、シェル24がステップS21でいずれかのアプリケーションプログラムからコマンドを受け付ける。ステップS22では、アプリケーション管理テーブル26を参照して、コマンド22に付加された識別コード23が、登録されたアプリケーションプログラム21の識別コード28と一致するかどうかを判断する。一致すれば、ステップS23に進み、コマンドの処理を実行する。一致しなければ、ステップS24に進み、エラー処理を実行し、そのコマンドの処理を拒絶する。なお、この例では、あらゆるコマンドは、シェル24でのみ受け付けられて、シェル24でのみ解釈されるという手順を確立しておくといよい。これで、極めてセキュリティの高いコンピュータシステムが確立できる。

【0046】図4の(a)はデータアクセスのセキュリティを高めるための管理方法を実現したシステムのブロック図であり、(b)はその動作フローチャートである。この実施例では、コンピュータで使用されるあらゆるメモリ、あるいは、保護を必用とするメモリ領域、例えば、特定のドライブに対するデータアクセスに上記の識別コードを利用する。図に示すように、データアクセス管理モジュール31は、メモリ32に記憶されたデータ33や、メモリ32に書き込まれるこれ以外のデータについてのアクセス管理を行う。このためにメモリ管理テーブル34を利用する。アクセスに利用されるデータは、図に示すように、アクセスコマンド35とデータ3

(8)

13

6と識別コード37とから構成される。メモリ管理テーブル34には、例えばアクセス管理をされるドライブ名38と識別コード39とを対応させて記憶しておく。この実施例では、メモリ管理テーブル34に登録されたドライブには、該当する識別コードを付加したデータしか読み書きできないようにする。

【0047】すなわち、アクセスコマンド35とデータ36と識別コード37とがデータアクセス管理モジュール31に入力すると、図の(b)に示すように、まずステップS31でそのコマンドを受け付ける。ステップS32で、データアクセス管理モジュール31は、メモリ管理テーブル34を参照する。そしてアクセスの対象がドライブ38であると判断すると、登録された識別コード39と、データ36に付加された識別コード37とを比較し、両者が一致するか判断する(ステップS32)。両者が一致すればメモリ32をアクセスするコマンドの実行を許可し、例えばデータの書き込みなどを許す(ステップS33)。一方、識別コードが一致しない場合には、ステップS30に進み、エラー処理を実行する。すなわち、データのアクセスを受け付けない。このデータアクセス管理モジュール31は、例えば、図3を用いて説明したシェルの一部の機能モジュールであってもよいし、全く独立に設けられたプログラムモジュールであってもよい。

【0048】以上のようにすれば、データに予め登録された識別コードが付加されていない場合には、該当するドライブのアクセスをすることができない。該当するドライブのデータを読み出すこともできないし、書き込むこともできない。従って、識別コードの管理を厳重にしておけば、ドライブ2はその識別コードを付加してアクセスをするアプリケーション以外のアクセスが完全に阻止される。従って、例えばネットワークを通じてコンピュータ中に入り込んだデータがメモリ上に無断で書き込まれるおそれがなく、極めてセキュリティの高いシステムを確立できる。

【0049】図5の(a)は上記のシステムをキャッシュカードなどに利用した管理方法の説明図で、(b)はその動作フローチャートである。図5において、カード41は、ICカードと呼ばれるキャッシュカードやクレジットカードであって、メモリを内蔵したカードである。このメモリに、既に説明したような所定の識別コードを割り付けられた識別コード応答モジュール42が記憶される。ATM(自動現金取引装置)43には、既に説明したような機能を持つ識別コード認証モジュール44が記憶されている。

【0050】このATM43は、例えば銀行などの窓口において預貯金の入出金に利用されている良く知られた装置である。図示しない多数のATM43は、いずれも、金融システムを管理するホストコンピュータ40と接続されている。なお、クレジットカードの場合には、

14

クレジットカード読み取り装置などがこのATMの代わりに利用される。カード41をATM43に装着すると、所定の手順によって認証処理がされ、よく知られた現金の入出金処理が実行される。このとき、上記識別コード応答モジュール42と識別コード認証モジュール44との間で、識別コードの認証処理が行われる。まず、カード41をATM43に装着すると(ステップS41)、カード41の利用者や口座番号などが、カードのメモリ中から自動的にATM43に読み取られる。ATM43の側では、ホストコンピュータ40の顧客管理用データベースを参照して、その利用者の識別コードに該当するデータを取得する。

【0051】識別コード認証モジュール44は、その識別コードを付加した問い合わせコマンドを出力して、カード41の識別コード応答モジュール42に問い合わせを行う。識別コードが一致している場合には、真正なカードであると判定され、認証が終了し(ステップS42)、カードの取引が実行される(ステップS43)。この処理の基本的な手順は既に図1のシステムの動作で説明したのと同様である。カード41にこのような機能を持たせると、識別コード応答モジュール42自体は、識別コードを発生させないため、カード41を調べても、ユーザーの識別コードを盗むことができない。

【0052】さらにこの実施例では、次のような手順によってカードを1回利用するたびに識別コードが変更されるように制御する。すなわち、カード41をATM43に装着して1回の取引を終了すると、ATM43は、新たな識別コード応答モジュールをカード41に書き込む。すなわち、カード41に当初記憶されていた識別コード応答モジュール42に代えて、これとは異なる別の識別コード応答モジュール45がカード41に記憶される(ステップS44、45)。当初の識別コード応答モジュール42には識別コードXが割り付けられていたとする。この場合取引が終了すると、カード41には、別の識別コードYが割り付けられた識別コード応答モジュール45が記憶される。ATM43の側では、識別コードをXからYに変更した旨を登録する。すなわち、次にこのカード41の利用者がATMを使用する場合には、識別コードYで認証処理が行われることになる。

【0053】上記のようにすれば、当初からカード41の中には、識別コードを直接読み取ることができるようなデータは、記録されていないから、カードをそのままコピーしない限り、そのカードを偽造できない。例えば、識別コード応答モジュール42は、識別コードを付加された問い合わせコマンドを受け入れたときに自分に割り付けられた識別コードと一致するかどうかを判断して、イエスあるいはノーという応答をするコンピュータプログラムである。従って、単純に外からデータを解析しても直接識別コードを読み取ることができないので、本人の識別コードを厳重に秘密に管理することができる

(9)

15

という効果がある。さらに、取引の都度識別コードが切り替えられるという方法を採用すれば、万一カード41の識別コード応答モジュール42をコピーして別のカードを用いてATMを操作しようとしても、そのときには識別コードが切り替わってしまっていて使用できない。故に、不正にコピーをしたカードは全く使用不能になる。すなわち、暗証番号を盗んだり、カードを不正にコピーしたものの使用を完全に阻止することが可能になる。

【0054】取引のたびにカードに新たな識別コードが割り付けられて、これまでの識別コードは無効になるという管理方法を採用する場合には、重複しないユニークな識別コードを発生する機構が必要になる。もちろん、利用者の利用者コードと組み合わせて使用されるのだから、完全に唯一無二の識別コードでなければならないというわけではない。例えば、国とか地域内ではユニークであるものとか、例えば、10年位の期間は重複が発生しないものというようにして識別コードを発生させてもよい。金融システムの場合、ホストコンピュータ40の部分にこうした識別コード発行機構を設けておき、ホストコンピュータ40によって管理される全てのATMに対しユニークな識別コードを供給するというシステムを組むことが好ましい。また、ホストコンピュータ40では常にどのユーザーがどの識別コードを使用しているかを管理し、切り替わっていく識別コードに応じて取引を実行できるようにするとよい。

【0055】また、図5の方法を図3や図4のコマンドに付加する識別コードに採用してもよい。例えば、アプリケーションプログラムが動作を開始するときに使用した識別コードは、動作が終了すると新たなものに更新される。同時にアプリケーション管理テーブルも書き換えられる。データのアクセス時に使用した識別コードは、一連のアクセス処理が終了すると新たなものに更新される。同時にメモリ管理テーブルも書き換えられる。識別コード応答モジュールを生成する識別コード認証モジュールが常にアプリケーションプログラムの動作やデータのアクセスを管理して、タイミングよく識別コードを更新していけば、きわめてセキュリティの高いプログラムやデータ管理が可能になる。

【0056】図6は本発明の変形例のブロック図である。図3の実施例では、シェル24がアプリケーション管理テーブルを参照して、登録された識別コードを付加しないコマンドの解釈を拒絶してオペレーティングシステムを保護した。図6の例では、この種の機能をカーネル側に持たせる。図6ではUNIX（登録商標）のオペレーティングシステムのシステムコールインタフェース61がアプリケーション管理テーブル56を参照する。即ち、アプリケーションプログラム21やライブラリ群51から識別コードを付加したコマンドがカーネル60のシステムコールインタフェース61に受けつけられ

16

る。システムコールインタフェース61は、アプリケーション管理テーブル56を参照する。アプリケーション管理テーブル56は、アプリケーションプログラム21やライブラリ群51の名称57と、それらの使用する識別コード58と対応させて登録したものである。システムコールインタフェース61はアプリケーションプログラム21やライブラリ群51が登録された識別コードを使用した場合は、コマンドをファイルサブシステム62やプロセス制御サブシステム63に伝え、それ以外の場合はエラー処理をするように制御する。これにより、図3の例と同様の管理が可能になる。図3のケースでも図6のケースでも、オペレーティングシステムにコマンドが達する前に識別コードをチェックして、不正なコマンドのオペレーティングシステムへの進入を阻止する事が出来る。即ち、オペレーティングシステムへ達する全てのコマンドの正当性を、そのコマンドに付加された識別コードを利用して判定する手段をコンピュータ中のいずれかの場所に設ければ、不正なコマンドのオペレーティングシステムへの進入を完全に阻止する管理が可能になる。もちろん、重要な機能を持つ特定のコマンドにのみ識別コードを付加するというルールを採用して、識別コードチェックの負荷を低減してもかまわない。

【0057】図7は、これまでとは別の管理方法の実施例で、プログラムやデータの不正コピー防止機能を強化したものの説明図である。図のCD-ROM70は、コンピュータプログラムや音楽その他様々なデータであって、コンピュータにインストールしようとする情報が記録された記憶媒体である。これらのデータをコンピュータ85にダウンロードしたり、インストールしたりする場合の、不正コピーを防止する。このために、CD-ROM70に、データ71とともに、応答モジュール72を記録しておく。データ71は、例えば、音楽とかコンピュータプログラムを、よく知られた圧縮形式で格納したものである。応答モジュール72は、認証モジュール73と暗証コード等の認証用データをやりとりする機能を持つコンピュータプログラムである。この認証手順は既に説明をした。

【0058】コンピュータ側には、認証モジュール73と解凍モジュール74とインストーラ75が動作できる状態で準備されている。解凍モジュール74は、圧縮処理されたデータ71を解凍処理する機能を持つプログラムである。インストーラ75は解凍されたデータをコンピュータ85の指定された部分に転送して記録する、良く知られたインストール処理を実行する機能を持つプログラムである。認証モジュール73は、ネットワーク80を通じてコンピュータ85に取り込まれる。このために、コンピュータ85には、配信要求モジュール81を設けておく。配信要求モジュール81は、認証モジュール配信用サーバ77に対して、例えば、対話式で認証モジュールのダウンロードを要求する機能を持つコンピ

(10)

17

ユータプログラムである。また、ネットワーク80に接続された認証モジュール配信用サーバ77には、どの利用者にどのような認証モジュールをいつ送信したかといった、認証モジュールの配信履歴データを記録する配信記録部76を設けておく。配信記録部76は、認証モジュール配信用サーバ77に接続された記憶装置などからなる。

【0059】このシステムでは、市販されたり、各種の方法で配布されるCD-ROM70だけを使って、コンピュータ85にデータやコンピュータプログラムをインストールすることができない。利用者は、あらかじめ一定の契約をして、配信要求モジュール81を操作して、認証モジュール配信用サーバ77に認証モジュール73の配信要求をし、コンピュータ85にダウンロードしておかなければならない。この認証モジュールが、CD-ROM70に記録されたデータ71のインストールを制御する。

【0060】この実施例では、正常にデータ71のインストールが終了すると、認証モジュール73はすみやかに無効化される。すなわち認証モジュール73を使用したインストール処理を、1回だけしかできないようにする。これにより認証モジュール73を盗み出してCD-ROM70に記録されたデータの不正コピーをする行為などを防止できる。なお、インストール後に何らかの障害が発生して、CD-ROMにより正規の利用者がデータ71の再インストールをしようとした時には、速やかに認証モジュール73を再配信できる体制が必要になる。そこで、配信要求モジュール81をコンピュータ85に残しておき、いつでも認証モジュール配信用サーバ77に配信を要求できるようにする。この場合に、認証モジュール73の配信履歴を配信記録部76に記録しておく。この配信記録は、利用者の認証モジュール73の不正利用を抑制する機能を持つ。認証モジュール73を要求できるのは、契約した利用者のみであるから、そのインストール先やインストールされたデータの管理と全てのインストール作業に、利用者が明確な責任を持つことになる。従って、利用者の知らない間に利用者のCD-ROMを不正にコピーしてデータやコンピュータプログラムをインストールするという問題が無くなる。

【0061】図8は、図7に示したシステムの具体的な動作フローチャートである。まず(a)に示すようにして、利用者は認証モジュールの配信を受ける。ステップS46において配信要求モジュール81が起動すると、認証モジュール配信用サーバ77が配信要求を受け付ける。次にステップS47において、配信記録部76の記録を更新する。そしてステップS48において認証モジュール配信用サーバ77は、認証モジュール73をネットワーク80を通じて利用者の端末に配信する。こうして認証モジュール73が利用者の端末上で起動できる状態になると、(b)に示すインストール処理が実行され

18

る。

【0062】はじめにステップS51において認証モジュールがダウンロードされると、ステップS52でインストール処理を開始する。CD-ROM70の応答モジュール72がコンピュータ85に転送されて起動し、認証モジュール73と暗証コードなどをやりとりして認証処理を実行する。認証をパスしない場合にはエラーが発生する。認証をパスするとステップS54に進む。そして解凍モジュール74がCD-ROM70に記録されたデータ71の解凍を行う。ステップS55では、インストーラ75がインストール処理を実行する。正常にインストールが終了すると、ステップS56において認証モジュール73の無効化が行われる。認証モジュール73の無効化方法は自由である。認証モジュール自身を消去する方法の他、認証モジュール73を動作させるためのパラメータを消去するといった方法も可能である。

【0063】図9は、銀行のキャッシュカードなどに本発明の方法を利用した場合の変形例説明図である。図の(a)はカードとATM(現金自動取引装置)の主要部ブロック図、(b)はその動作説明図である。(a)に示すように、カード側には識別コード発生モジュール90と識別コードレジスタ91が設けられている。識別コード発生モジュール90は、カードに搭載されたコンピュータ上で動作するコンピュータプログラムである。識別コードレジスタ91はカードのメモリ中の記憶領域に設けられる。また、ATM側にも同じように識別コード発生モジュール95と識別コードレジスタ96が設けられている。識別コード発生モジュール95は、ATMのコンピュータ上で動作するコンピュータプログラムである。識別コードレジスタ96はATMのメモリ中の記憶領域に設けられる。

【0064】識別コード発生モジュール90は、認証処理開始直前にパスワード92を入力すると、認証モジュール99が処理を開始する前に、識別コードレジスタ91に記憶された識別コードを読み出して、新たな識別コードを発生する機能を持つ。識別コード発生モジュール95も全く同様の機能を持ち、パスワード92が入力した時に、識別コードレジスタ96に記憶された識別コードを利用して新たな識別コードを発生する。識別コード発生モジュール90と識別コード発生モジュール95の機能は全く同一であって、同一のパスワードと同一の識別コードを入力すると、同一の新たな識別コードを発生する。従って、この図に示すような状態で、顧客がATMにカードを装着してパスワード92を入力すると、カード側とATM側で同時に新たな識別コードを発生させる。このとき、カード側とATM側で全く同一の識別コードが得られる。これが認証モジュール99で比較され、認証処理が行われる。すなわち、カード側で識別コード発生モジュール90が発生した識別コードとATM側で識別コード発生モジュール95が発生した識別コード

(11)

19

ドとが一致すれば、認証処理が正常に終了したとして現金の取引などが進められる。その他の場合には、エラー処理が行われる。

【0065】この実施例では次のような非常に重要な効果が得られる。まず、カード側もATM側も、識別コードレジスタ91と96に、前回使用された識別コードを記憶しているものの、次の取引に使用する識別コードはどこにも記憶していない。次の取引では、識別コードレジスタ91と96に記憶された識別コードと利用者の入力したパスワードを用いて生成した新たな識別コードが、認証に利用される。このため例えば、カード側に記録された情報を盗み取った第三者が識別コードレジスタ91に記憶された識別コードを使用して不正な取引を行おうとしても、ATMは反応しない。識別コード発生モジュール90を実際に動作させなければ、取引に必要な識別コードが得られない。

【0066】しかも、カードを1回使うたびに、即ち、1回の認証処理ごとに全く新たな識別コードを発生させて利用するので、第三者が識別コードを直接コピーして使用することができない。新たな識別コードを発生させるのに、直前の認証処理で発生させた識別コードだけでなく、ユーザの入力するパスワードも利用するようにすれば、よりセキュリティの高い運用ができる。また、図の(b)に示すように、カード101とまったく同一の構成のカードを第三者が製造したとする。このとき識別コードもカード101からカード102にコピーしたとする。この状態で、利用者のパスワードも盗んで第三者がすぐにカードを使用するとそのカードで有効な取引ができる。

【0067】しかし、正規の利用者がカード101を使用してATM100を動作させると、その時点で識別コードレジスタ91、96に記憶された識別コードの内容が変化してしまう。すなわち1回目、2回目、3回目というようにどんどん識別コードの内容が変化してしまう。従って、以前に識別コードを不正に入手した第三者がその後カード102を使用しても、その時点では既に識別コードが変化しており、カード102は使用できない。このように単に識別コードを毎回切り換えるといった処理を行うだけでなく、上記のようにカード側とATM側とでそれぞれ新たな識別コードを発生するモジュールを設け、新たな識別コードをその都度利用して認証処理を行うと、極めて安全性の高い取引ができる。

【0068】図10は、図9に示したカードを使用したATMの動作を説明するためのフローチャートである。まず、ステップS61において、ATM100にカード101が挿入されると、ステップS62でパスワードの入力が要求される。パスワードが入力されると、カード側とATM側とでそれぞれ識別コード発生モジュールが起動する。カード側ではステップS63で旧識別コードが読み取られ、ステップS64で新たな識別コードが発

20

生する。またATM側でも同じようにステップS65において旧識別コードが読み取られ、ステップS66で新識別コードが発生する。その後ステップS67で、カード側で発生した識別コードとATM側で発生した識別コードとの比較処理を行う。この処理は、ATM内で動作する認証モジュール99が実行する。ステップS68で両識別コードが一致したと判断すると、ステップS69に進み、取引を開始する。また、一致しなかった場合には、カードは返却し、エラー処理を行う(ステップS70)。

【0069】図11は、本発明の方法をコンピュータのオペレーティングシステムに使用した場合の別の実施例を示すブロック図である。既に説明したように、コンピュータのオペレーティングシステム111に任意のアプリケーション110をインストールし、これを動作させる場合に、管理テーブル113を用意して、アプリケーション114に対応する識別コード115を登録しておけば、未登録のアプリケーションがオペレーティングシステム111上で動作するのを禁止できる。即ち、正規に登録されたアプリケーションのコマンドのみをオペレーティングシステム111に渡すようにする。これにより、オペレーティングシステム111が全く管理していないアプリケーションからのデータ書き込み等の処理を排除し、コンピュータの正常動作を確保する。また、不正に外部からアクセスされたり、コンピュータウィルスにより不正な処理が行われるのを排除できる。

【0070】このような厳格な管理は、限定されたアプリケーションしか使用しない、例えば、銀行などのシステムに適する。しかしながら、個人用のパーソナルコンピュータのように、インターネットに接続して様々なデータを利用し、かつ安全にアプリケーションプログラムを使用したいといった環境には不向きである。図の

(b)に示すものは、(a)に示すものを改良した例を示す。図に示すように、監視モジュール117は、

(b)に示したものと同様に、アプリケーション118とオペレーティングシステム119との間に介在する。しかしながらネットワーク200に接続されたネットワークインターフェイス201の動作は、この監視モジュール117の監視外に置く。そして、記憶領域202に対しては、ネットワークインターフェイス201が自由にデータの書き込みなどを行えるようにする。なお、不正なデータやプログラムがメモリの任意の領域に書き込まれるのを防止するために、ネットワークインターフェイス201がデータを書き込むことのできる記憶領域を限定しておいても構わない。

【0071】こうして、ネットワーク200と接続をして一定の処理を行うための領域202を、監視モジュールの管理外におく。従って、例えば、ブラウザとその閲覧履歴を記憶するテンポラリファイルと、HTMLプロトコル上で動作するアプリケーションの動作には制約を

(12)

21

加えない。一方、例えば、ネットワーク200を通じてデータやアプリケーションプログラムをダウンロードして、オペレーティングシステム119により動作させようとする場合には、認証登録モジュール203が領域202から必要なデータを取り込み、管理テーブル113に登録する。この実施例によって、ネットワークと自由に通信を行い、自由にデータを取り込み、自由にアプリケーションをダウンロードする環境が得られる。

【0072】なお、各図に示した各機能ブロックは、それぞれ別々のプログラムモジュールにより構成してもよいし、一体化したプログラムモジュールにより構成してもよい。また、これらの機能ブロックの全部または一部を論理回路によるハードウェアで構成しても構わない。また、各プログラムモジュールは、既存のアプリケーションプログラムに組み込んで動作させてもよいし、独立のプログラムとして動作させてもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばCD-ROMのようなコンピュータで読み取り可能な記録媒体に記録して、インストールして利用することができる。また、ネットワークを通じてコンピュータのメモ

【図面の簡単な説明】

【図1】本発明のプログラムやデータの管理方法を実施するためのシステムブロック図である。

【図2】上記のアプリケーションプログラム識別コード応答モジュール11とインストーラ12と識別コード認証モジュール13の動作を示すシーケンスチャートである。

【図3】(a)は、コンピュータにインストールされたアプリケーションプログラムの動作を制限してセキュリティを高める管理方法の説明図で、(b)はその動作フ

22

【図4】(a)はデータアクセスのセキュリティを高めるための管理方法を実現したシステムのブロック図であり、(b)はその動作フローチャートである。

【図5】(a)は上記のシステムをキャッシュカードなどに利用した管理方法の説明図で、(b)はその動作フローチャートである。

【図6】本発明の変形例のブロック図である。

【図7】これまでとは別の管理方法の実施例で、プログラムやデータの不正コピー防止機能を強化したものの説明図である。

【図8】図7に示したシステムの具体的な動作フローチャートである。

【図9】銀行のキャッシュカードなどに本発明の方法を利用した場合の変形例説明図である。図の(a)はカードとATM(現金自動取引装置)の主要部ブロック図、(b)はその動作説明図である。

【図10】図9に示したカードを使用したATMの動作を説明するためのフローチャートである。

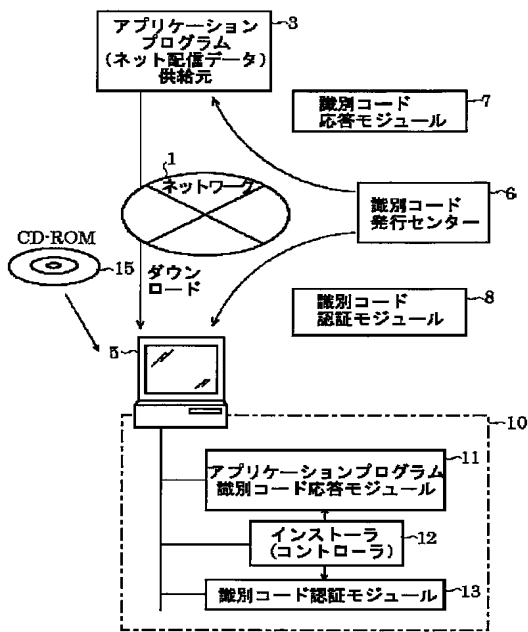
【図11】本発明の方法をコンピュータのオペレーティングシステムに使用した場合の別の実施例を示すブロック図である。

【符号の説明】

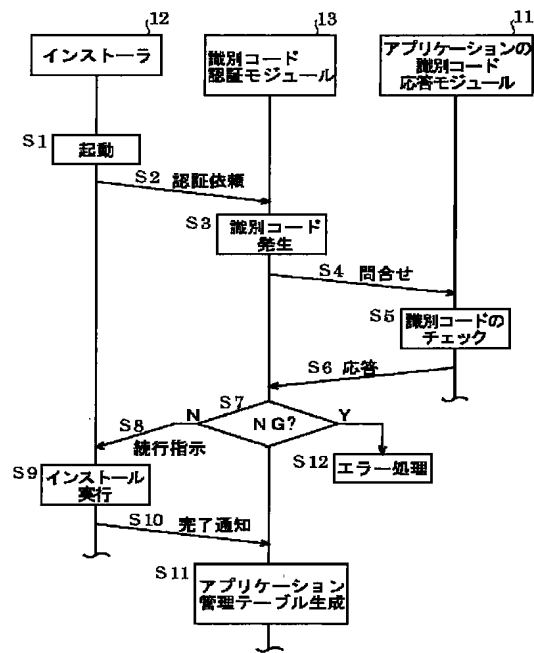
- 1 ネットワーク
- 3 アプリケーションプログラム供給元
- 5 端末
- 6 識別コード発行センター
- 7 識別コード応答モジュール
- 8 識別コード認証モジュール
- 11 アプリケーションプログラム識別コード応答モジュール
- 12 インストーラ
- 13 識別コード認証モジュール

(13)

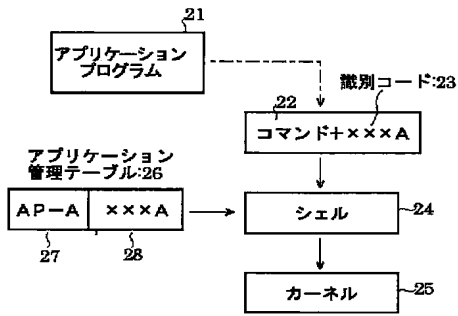
【図1】



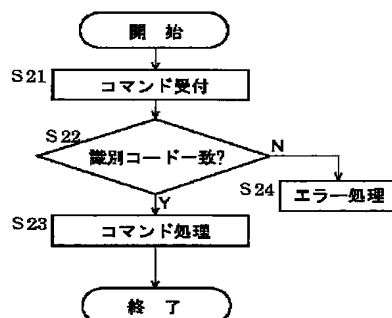
【図2】



【図3】

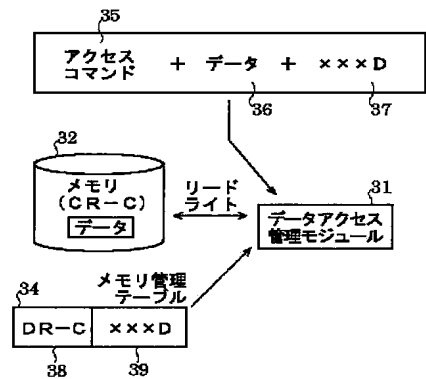


(a)

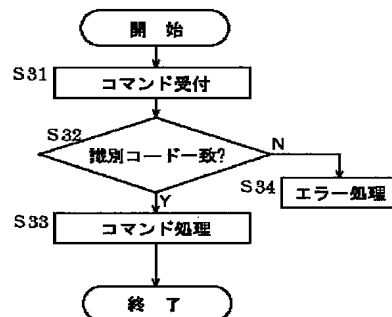


(b)

【図4】



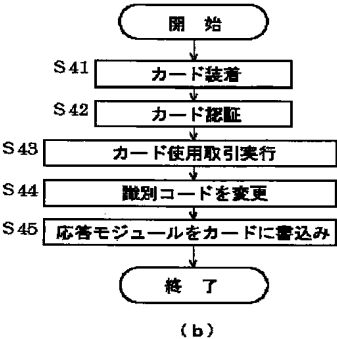
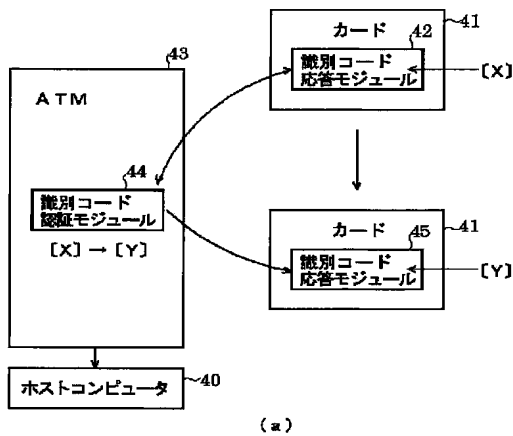
(a)



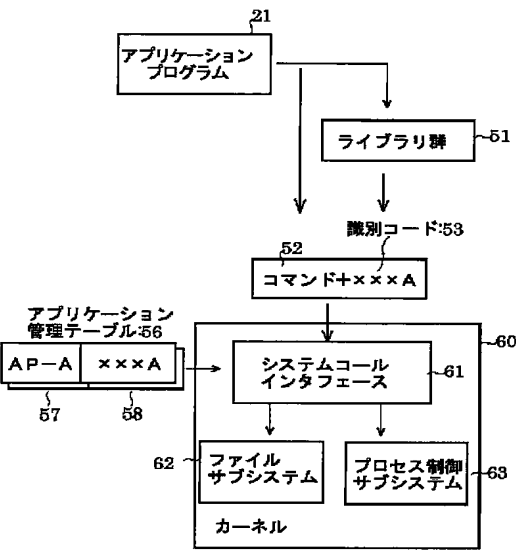
(b)

(14)

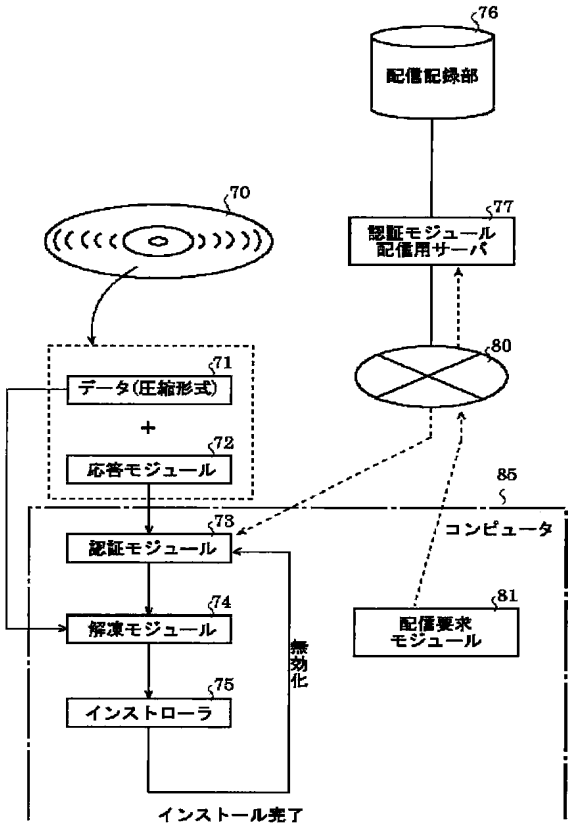
【図5】



【図6】

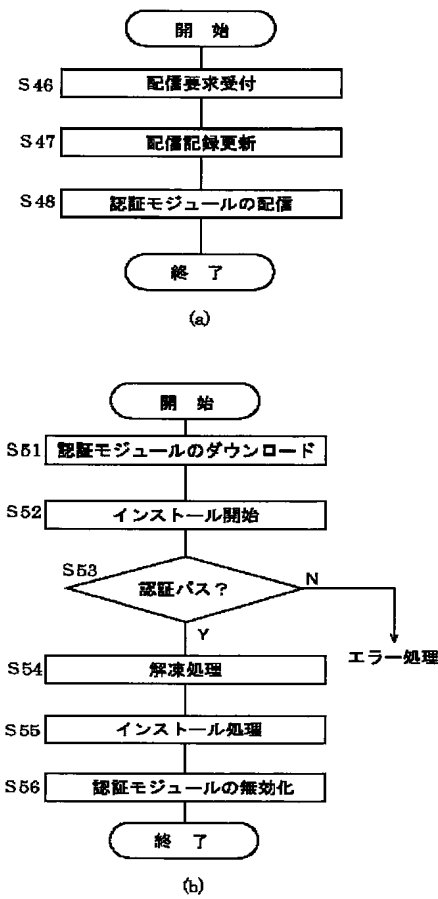


【図7】

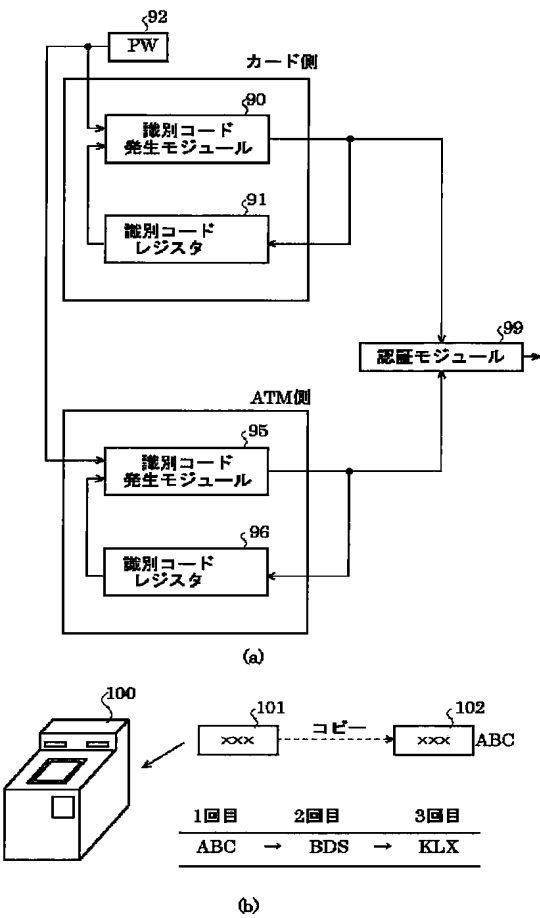


(15)

【図 8】

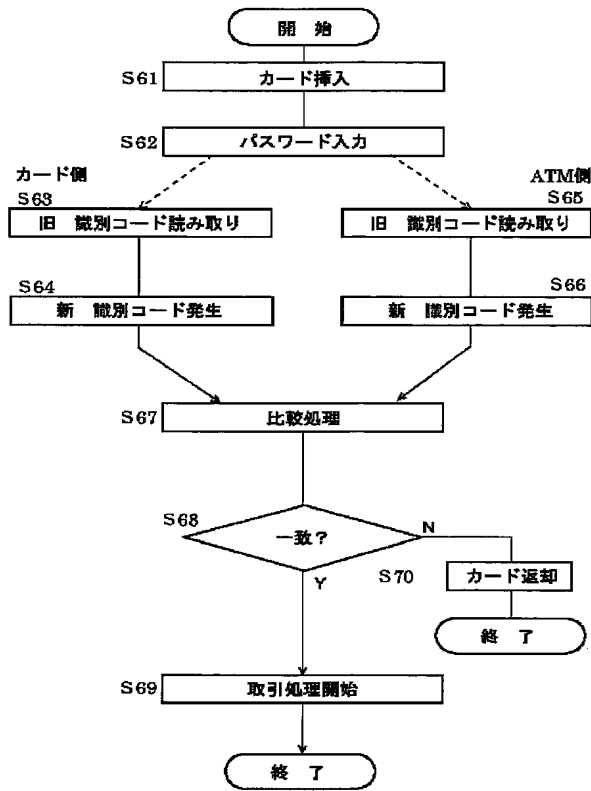


【図 9】



(16)

【図10】



【図11】

